EUROPESE
COMMISSIE

Brussel, 24.7.2019
COM(2019) 372 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

over de onderlinge koppeling van nationale gecentraliseerde automatische mechanismen (centrale registers of centrale elektronische systemen voor gegevensontsluiting) van de lidstaten voor bankrekeningen

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

over de onderlinge koppeling van nationale gecentraliseerde automatische mechanismen (centrale registers of centrale elektronische systemen voor gegevensontsluiting) van de lidstaten voor bankrekeningen

1. Inleiding

Volgens artikel 32 bis van antiwitwasrichtlijn 2015/849/EU[1] moeten de lidstaten uiterlijk 10 september 2020 beschikken over gecentraliseerde automatische mechanismen, zoals centrale registers of centrale elektronische systemen voor gegevensontsluiting, die de identificatie mogelijk maken van alle natuurlijke of rechtspersonen die houder zijn van of zeggenschap hebben over betaalrekeningen, bankrekeningen en kluizen. In de antiwitwasrichtlijn is een minimumpakket aan informatie vastgesteld dat in dergelijke gecentraliseerde mechanismen moet zijn opgenomen. In de richtlijn is tevens bepaald dat de financiële inlichtingeneenheden onmiddellijk en ongefilterd toegang tot die informatie moeten hebben, terwijl ook andere bevoegde autoriteiten met het oog op het nakomen van hun verplichtingen uit hoofde van de antiwitwasrichtlijn toegang moeten hebben. Richtlijn 2019/1153 ter vergemakkelijking van het gebruik van financiële en andere informatie[2] verplicht de lidstaten ertoe de nationale autoriteiten met bevoegdheden tot het voorkomen, opsporen, onderzoeken of vervolgen van strafbare feiten aan te wijzen die rechtstreeks, onmiddellijk en ongefilterd toegang moeten hebben tot het minimumpakket aan informatie in die gecentraliseerde mechanismen. Die bevoegde autoriteiten omvatten ten minste de bureaus voor de ontneming van vermogensbestanddelen.

De toegang door bevoegde autoriteiten tot centrale registers van bankrekeningen of systemen voor gegevensontsluiting zal een belangrijk wapen zijn in de strijd tegen witwassen, daarmee verband houdende basisdelicten en terrorismefinanciering, alsook in de bestrijding van ernstige misdrijven in het algemeen. Indachtig de doelstellingen van de antiwitwasrichtlijn en de richtlijn ter vergemakkelijking van het gebruik van financiële en andere informatie, vergemakkelijkt een toekomstige, EU-brede onderlinge koppeling van registers van bankrekeningen en systemen voor gegevensontsluiting de grensoverschrijdende samenwerking tussen de bevoegde autoriteiten die betrokken zijn in de strijd tegen witwassen, terrorismefinanciering en andere ernstige misdrijven.

[1] Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PB L 141 van 5.6.2015, blz. 73).

[2] Richtlijn (EU) 2019/1153 van het Europees Parlement en de Raad van 20 juni 2019 tot vaststelling van regels ter vergemakkelijking van het gebruik van financiële en andere informatie voor het voorkomen, opsporen, onderzoeken of vervolgen van bepaalde strafbare feiten (PB L 186 van 11.7.2019, blz. 122).

Volgens artikel 32 bis, lid 5, van de antiwitwasrichtlijn moet de Commissie de voorwaarden en de technische kenmerken en procedures beoordelen die nodig zijn voor een veilige en doeltreffende koppeling van de gecentraliseerde automatische mechanismen. In dit verslag worden daarom de diverse IT-oplossingen op EU-niveau – reeds in bedrijf of nog in ontwikkeling – beoordeeld die als model kunnen dienen voor de mogelijke koppeling van gecentraliseerde mechanismen. Voor het bewerkstelligen van een koppeling is een wetgevingsinstrument vereist.

Dit verslag moet worden beschouwd in samenhang met het verslag van de Commissie over de supranationale risicobeoordeling,[3] het verslag van de Commissie over financiële inlichtingeneenheden[4] en het verslag van de Commissie over de beoordeling van recente vermeende gevallen van het witwassen van geld waarbij EU-kredietinstellingen betrokken zijn[5]. Deze verslagen worden gelijktijdig gepresenteerd.

2. Stand van zaken

2.1. Centrale registers of systemen voor gegevensontsluiting voor bankrekeningen in de lidstaten

Momenteel[6] zijn in vijftien lidstaten gecentraliseerde mechanismen met bankrekeninginformatie in gebruik[7]. Uit de antwoorden van de lidstaten spreekt een lichte voorkeur voor de technische oplossing van het centraal register: terwijl 17 lidstaten nu of binnenkort beschikken over centrale registers hebben negen lidstaten verklaard dat zij centrale systemen voor gegevensontsluiting hebben of die overwegen[8]. Er bestaat ook een voorkeur voor systemen die, naast het minimumpakket aan informatie over het profiel van de

[3] Verslag van de Commissie aan het Europees Parlement en de Raad over de beoordeling van risico's op het gebied van witwassen en terrorismefinanciering die van invloed zijn op de interne markt en verband houden met grensoverschrijdende activiteiten (COM(2019) 370).

[4] Verslag van de Commissie aan het Europees Parlement en de Raad waarin het kader voor de samenwerking tussen de financiële inlichtingeneenheden wordt beoordeeld (COM(2019) 371).

[5] Verslag van de Commissie aan het Europees Parlement en de Raad over de beoordeling van recente vermeende gevallen van het witwassen van geld waarbij EU-kredietinstellingen betrokken zijn (COM(2019) 373).

[6] De informatie in dit gedeelte is gebaseerd op de antwoorden van de lidstaten op een speciale vragenlijst die hun in maart 2019 is toegestuurd, op de informatie die tijdens de door de Commissie georganiseerde workshop over omzetten op 1 april 2019 werd ontvangen en op bijlage 7 van de effectbeoordeling bij het voorstel voor een richtlijn van het Europees Parlement en de Raad tot vaststelling van regels ter vergemakkelijking van het gebruik van financiële en andere informatie voor het voorkomen, opsporen, onderzoeken of vervolgen van bepaalde strafbare feiten, en tot intrekking van Besluit 2000/642/JBZ van de Raad (SWD(2018) 114 final).

[7] België, Bulgarije, Tsjechië, Duitsland, Griekenland Spanje, Frankrijk, Kroatië, Italië, Letland, Litouwen, Oostenrijk, Portugal, Roemenië en Slovenië. Slowakije beschikt over een centraal elektronisch systeem voor gegevensontsluiting dat op dit moment echter uitsluitend voor magistraten toegankelijk is.

[8] Finland telt in beide categorieën mee aangezien dit land op het punt staat een systeem in gebruik te nemen dat van beide oplossingen gebruikmaakt. Een centraal register verzamelt en bewaart de relevante informatie in één centrale databank, terwijl een centraal elektronisch systeem voor gegevensontsluiting uit een centraal IT-portaal bestaat dat informatie ophaalt bij diverse onderliggende databanken (die onder andere door financiële instellingen worden beheerd).

rekeninghouder als bedoeld in artikel 32 bis, lid 5, van de vijfde antiwitwasrichtlijn, extra gegevens bevatten (11 tegen 6 antwoorden)[9].

2.2. EU-systemen voor de onderlinge koppeling van nationale decentrale elektronische databanken

Er bestaan diverse EU-projecten die zorgen voor de onderlinge koppeling van decentrale nationale elektronische databanken in de hele EU[10]. De volgende IT-systemen worden in het kader van dit verslag als relevant beschouwd:

Het Europees Strafregister Informatiesysteem (Ecris) werd in april 2012 in gebruik genomen met de bedoeling om de uitwisseling van informatie over strafregisters in de EU te verbeteren[11]. Alle lidstaten zijn op dit moment met Ecris verbonden. Ecris zorgt ervoor dat informatie over strafrechtelijke veroordelingen op uniforme, snelle en verenigbare wijze tussen de lidstaten wordt uitgewisseld en biedt rechters en openbare aanklagers eenvoudig toegang tot uitvoerige informatie over het strafrechtelijk verleden van betrokkenen[12].

Het Europees voertuig- en rijbewijsinformatiesysteem (Eucaris) verbindt landen met elkaar zodat zij informatie over voertuigen en rijbewijzen kunnen uitwisselen, alsook andere gegevens die betrekking hebben op vervoer. Eucaris is een mechanisme dat de autoriteiten in de Unie die belast zijn met de registratie van voertuigen en rijbewijzen, met elkaar verbindt en met behulp waarvan de nationale contactpunten van de lidstaten informatie over de voertuigeigenaren en motorrijtuigenverzekeringen kunnen uitwisselen[13].

De EU-brede onderlinge koppeling van insolventieregisters (IRI), die twee verschillende projecten omvat. De eerste versie van het systeem (IRI 1.0) is sinds juli 2014 beschikbaar op het Europees e-justitieportaal[14]. Het is ontwikkeld als een proefproject[15] waaraan bepaalde

---

[9] Volgens de antwoorden van de lidstaten kan het bij dergelijke aanvullende informatie gaan om informatie over financiële contracten die door de rekeninghouder zijn afgesloten of over met die rekening verrichte transacties.

[10] Gecentraliseerde IT-systemen met afzonderlijke databanken op EU-niveau, zoals het Schengeninformatiesysteem en het Visuminformatiesysteem, worden buiten de beoordeling gelaten aangezien dergelijke systemen niet verenigbaar zijn met reeds bestaande nationale centrale databanken.

[11] Kaderbesluit 2009/315/JBZ van de Raad van 26 februari 2009 betreffende de organisatie en de inhoud van de uitwisseling van strafregisters tussen de lidstaten en Besluit 2009/316/JBZ van de Raad van 6 april 2009 betreffende de oprichting van het Europees Strafregister Informatiesysteem (ECRIS) overeenkomstig artikel 11 van Kaderbesluit 2009/315/JBZ, op dit moment gewijzigd bij Richtlijn (EU) 2019/884 van het Europees Parlement en de Raad van 17 april 2019 betreffende de uitwisseling van informatie over onderdanen van derde landen en betreffende het Europees Strafregisterinformatiesysteem (Ecris).

[12] In april 2019 is een nieuw wetgevingskader vastgesteld om Ecris aan te vullen met een mechanisme ten behoeve van de doeltreffende uitwisseling van strafregistergegevens over onderdanen van derde landen die op het EU-grondgebied zijn veroordeeld. Het Europees Strafregister Informatiesysteem voor onderdanen van derde landen (Ecris-TCN) betreft een centraal hit/no hit-systeem dat alleen identiteitsgegevens van veroordeelde onderdanen van derde landen bevat en een vermelding van de lidstaat waarin zij eerder zijn veroordeeld. Bij een treffer moet de verzoekende lidstaat via het bestaande Ecris-systeem informatie over de veroordeling opvragen bij de in Ecris-TCN vermelde lidstaat/lidstaten.

[13] De rechtsgrondslagen voor de Prüm-dienst zijn: Besluit 2008/615/JBZ van de Raad van 23 juni 2008 inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van terrorisme en grensoverschrijdende criminaliteit en Besluit 2008/616/JBZ van de Raad betreffende de uitvoering van Besluit 2008/615/JBZ.

[14] https://beta.e-justice.europa.eu/246/NL/bankruptcy_amp_insolvency_registers__search_for_insolvent_firms_in_the_eu?init=true

lidstaten vrijwillig deelnemen[16]. De tweede versie (IRI 2.0) is gebaseerd op Verordening (EU) 2015/848 betreffende insolventieprocedures en zal de nationale insolventieregisters van alle lidstaten (met uitzondering van Denemarken) met elkaar verbinden. Alle lidstaten moeten de koppeling uiterlijk in juni 2021 geregeld hebben. IRI 1.0 is gebaseerd op gestandaardiseerde beveiligde berichten van webdiensten (SOAP over HTTPS), terwijl IRI 2.0 ook gegevensuitwisseling ondersteunt door gebruik te maken van de bouwsteen eDelivery van de financieringsfaciliteit voor Europese verbindingen (Connecting Europe Facility; CEF)[17].

Het Business Registers Interconnection System (BRIS) betreft de koppeling van bedrijfsregisters, met behulp waarvan bedrijfsregisters grensoverschrijdende berichten kunnen uitwisselen over fusies en bijkantoren, en de gebruikers van het e-justitieportaal meertalige informatie over ondernemingen in de EU kunnen verkrijgen. Het systeem is sinds juni 2017 in bedrijf, overeenkomstig Richtlijn 2012/17/EU wat de koppeling van centrale, handels- en vennootschapsregisters betreft[18]. BRIS maakt voor de uitwisseling van gestandaardiseerde berichten gebruik van de bouwsteen eDelivery van de financieringsfaciliteit voor Europese verbindingen. Het is een decentraal systeem met een centrale component (het Europees centraal platform) die bedrijfsnamen en registratienummers opslaat en indexeert.

De onderlinge koppeling van kadasters (Land Registers Interconnection; LRI) is een lopend project op vrijwillige basis[19] dat binnen het Europees e-justitieportaal één toegangspunt tot de kadasters van deelnemende EU-landen wil aanbieden. Volgens planning wordt het in het tweede kwartaal van 2020 in gebruik genomen.

Het project Eigendoms- en zeggenschapsstructuren van Europese ondernemingen (European Business Ownership and Control Structures; Ebocs) wordt uitgevoerd door de European Business Registries Association, met financiële ondersteuning uit het jaarlijks werkprogramma 2016 en 2018 van het Fonds voor interne veiligheid Politie (ISF). Het Ebocs-platform biedt vereenvoudigde en geharmoniseerde toegang tot bedrijfsregistergegevens over eigendoms- en zeggenschapsstructuren van ondernemingen ten behoeve van financiële analyse en onderzoek. Het voorziet tevens in kaarten waarop de geaggregeerde zoekresultaten zijn gevisualiseerd. Opgemerkt wordt dat de EU niet de intellectuele eigendomsrechten van dit systeem bezit.

Het systeem e-Codex (e-justice Communication via Online Data Exchange) vergemakkelijkt beveiligde communicatie in civiele en strafzaken aan de hand van een decentraal systeem

---

[15] Het proefproject werd uitgevoerd op basis van en verder uitgewerkt in het Meerjarenactieplan 2009-2013 voor de Europese e-justitie (PB C 75, 31.3.2009, blz. 1) en het Meerjarenactieplan 2014-2018 voor de Europese e-justitie (PB C 182, 14.6.2014, blz. 2).

[16] Momenteel nemen Tsjechië, Duitsland, Estland, Italië, Letland, Nederland, Oostenrijk, Roemenië en Slovenië hieraan deel.

[17] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

[18] Richtlijn 2012/17/EU van het Europees Parlement en de Raad van 13 juni 2012 tot wijziging van Richtlijn 89/666/EEG van de Raad en Richtlijnen 2005/56/EG en 2009/101/EG van het Europees Parlement en de Raad wat de koppeling van centrale, handels- en vennootschapsregisters betreft (PB L 156 van 16.6.2012).

[19] Er bestaat geen rechtsgrondslag voor de koppeling, maar LRI fungeert als een systeem op vrijwillige basis waaraan lidstaten naar keuze kunnen deelnemen.

voor de uitwisseling van grensoverschrijdende elektronische berichten in de rechtsruimte[20]. Momenteel bevordert e-Codex de elektronische communicatie tussen burgers en rechtbanken en tussen de overheidsdiensten van de lidstaten bij het proefproject voor de Europese betalingsbevelprocedure en de Europese procedure voor geringe vorderingen. Op het gebied van het strafrecht vormt e-Codex tevens de voorkeursoplossing voor een digitaal uitwisselingssysteem voor elektronisch bewijsmateriaal[21] en voor elektronische uitwisselingen in het kader van het Europees onderzoeksbevel (EOB) en wederzijdse rechtshulpverdragen.

3. Voornaamste parameters

3.1. Toegangsvoorwaarden voor gebruikers

Een blik op de bestaande systemen leert dat de toegankelijkheid van het gebruikerssysteem dat met het gekoppelde IT-systeem communiceert wordt bepaald door het doel waarvoor het is opgezet. Het systeem is openbaar toegankelijk indien de koppeling is gemaakt met als doel de transparantie van informatie voor ondernemingen in de interne markt te vergroten (BRIS, IRI). De toegang is beperkt indien de koppeling moet zorgen voor betere grensoverschrijdende samenwerking tussen bevoegde autoriteiten ten behoeve van de rechtshandhaving of openbare administratieve doeleinden, zoals in het geval van Ecris of de Prüm-dienst van Eucaris[22].

De functie "Een bedrijf zoeken" van BRIS is in het e-justitieportaal voor iedereen toegankelijk, maar de infrastructuur voor berichten is voor nationale bedrijfsregisters momenteel wettelijk beperkt. Bij IRI is de informatie via de zoekinterface openbaar toegankelijk en hebben lidstaten alleen in het kader van "insolventieprocedures voor consumenten" de mogelijkheid om de toegang te beperken tot verzoekers met een rechtmatig belang. Ecris is alleen toegankelijk voor de aangewezen centrale autoriteiten van de lidstaten. Ook de diensten van Eucaris zijn via de aangewezen nationale contactpunten toegankelijk voor overheidsinstanties. Voor Ebocs geldt dat de toegang beperkt is tot de deelnemende instanties voor criminaliteitsbestrijding.

Systeem	Openbaar toegankelijk	Beperkte toegang	Opmerkingen
BRIS	Ja		De functie "Een bedrijf zoeken" van BRIS is in het e-justitieportaal voor iedereen toegankelijk,

[20] Het systeem e-Codex bestaat uit een pakket softwareproducten (eDelivery van de CEF en de e-Codex-connector) dat kan worden gebruikt voor het instellen van een toegangspunt op nationaal niveau ten behoeve van dergelijke beveiligde communicatie. Het is geen systeem dat nationale databanken of registers aan elkaar koppelt, maar een communicatie-infrastructuur die zorgt voor beveiligde communicatie en informatie-uitwisseling tussen nationale IT-systemen en als zodanig van belang wordt beschouwd voor de beoordeling in dit verslag. e-Codex is tussen 2010 en 2016 door 21 lidstaten ontwikkeld en andere landen/gebieden en organisaties hebben daaraan deelgenomen.

[21] Ingesteld naar aanleiding van de conclusies van de Raad over het verbeteren van de strafrechtspleging in de cyberruimte van 9 juni 2016.

[22] Hoewel diverse autoriteiten toegang hebben tot Eucaris, regelt de Prüm-dienst van Eucaris de toegang door rechtshandhavingsinstanties.

			maar de infrastructuur voor berichten is voor nationale bedrijfsregisters momenteel wettelijk beperkt
IRI	Ja		
Ecris		Ja	Voor centrale autoriteiten van de lidstaten die speciaal met deze taak zijn belast
Eucaris		Ja	Voor de nationale contactpunten van Eucaris, via welke overheidsinstanties toegang kunnen verkrijgen, afhankelijk van de rechtsgrondslag van de samenwerking
Ebocs		Ja	Voor instanties voor criminaliteitsbestrijding die deelnemen aan het project
LRI	Ja*		De geavanceerde functies zullen alleen voor erkende rechtsbeoefenaren beschikbaar zijn

Tabel 1: Toegankelijkheid van het gebruikerssysteem dat met het gekoppelde IT-systeem communiceert

Volgens de antiwitwasrichtlijn zijn de gecentraliseerde mechanismen voor bankrekeningen bedoeld om witwassen en terrorismefinanciering beter te kunnen bestrijden en is de toegang ertoe beperkt tot bepaalde overheidsinstanties. In de richtlijn ter vergemakkelijking van het gebruik van financiële en andere informatie wordt het gebruiksdoel van de informatie in de gecentraliseerde mechanismen verbreed tot ernstige criminaliteit en de toegangsrechten verruimd tot de aangewezen bevoegde autoriteiten. Welke binnenlandse autoriteiten rechtstreeks toegang hebben tot de nationale registers, ten slotte, wordt bepaald door de lidstaat die de registers beheert. Dit kan verschillen veroorzaken, aangezien sommige typen autoriteit in de ene lidstaat wel en in de andere lidstaat geen toegang krijgen. Bij een grensoverschrijdende uitwisseling via het EU-brede verbindingssysteem kan dat tot een situatie leiden waarin een autoriteit informatie opvraagt uit het register van een andere lidstaat, terwijl die zoekopdracht aan een soortgelijke autoriteit wordt geweigerd.

Eén mogelijkheid is om de autoriteiten waaraan overeenkomstig de antiwitwasrichtlijn en de richtlijn ter vergemakkelijking van het gebruik van financiële en andere informatie rechtstreekse toegang tot de gecentraliseerde mechanismen zal worden verleend, ook toegang tot het verbindingsplatform te geven. Een andere mogelijkheid is om in alle lidstaten toegangsrechten tot het verbindingssysteem toe te kennen aan dezelfde typen autoriteit, wat bewerkstelligd kan worden door middel van een geharmoniseerde en gesloten lijst op EU-niveau met de typen autoriteit die overeenkomstig het doel van de toegang tot de informatie zijn gespecificeerd.

Er zijn uitvoerige bepalingen inzake de voorwaarden voor toegang en doorzoekingen door bevoegde nationale autoriteiten nodig indien de koppeling wordt uitgebreid naar alle autoriteiten waaraan op dit moment krachtens de nationale wetgeving toegang is verleend. In dit verband moet gewezen worden op het feit dat in de richtlijn ter vergemakkelijking van het gebruik van financiële en andere informatie strikte voorwaarden zijn vastgesteld voor de toegang tot en het doorzoeken van de bankrekeninginformatie in de automatische gecentraliseerde mechanismen door de bevoegde autoriteiten die op nationaal niveau zijn aangewezen. Een dergelijke voorwaarde is bijvoorbeeld dat alleen aan medewerkers van alle

* Nog niet operationeel.

bevoegde autoriteiten die daartoe specifiek zijn aangewezen en gemachtigd toegang tot de registers en systemen voor gegevensontsluiting wordt verleend. Een andere maatregel ter verkleining van de risico's van verruimde toegangsrechten voor de aangewezen nationale autoriteiten kan zijn om het soort in het verbindingssysteem beschikbare informatie te beperken tot het minimumpakket dat betrekking heeft op het profiel van de rekeninghouder, zoals bepaald in artikel 32 bis, lid 3, van de antiwitwasrichtlijn.

Wat het soort informatie betreft, is in artikel 32 bis, lid 3, van de antiwitwasrichtlijn gedefinieerd welke informatie alle gecentraliseerde mechanismen moeten bevatten, zoals de rekeninghouder, de IBAN-nummers van de bankrekeningen, en de kluizen die een kredietinstelling op het nationale grondgebied heeft. Artikel 32 bis, lid 4, van de richtlijn voorziet echter in de mogelijkheid dat lidstaten andere informatie in de registers opnemen die essentieel wordt geacht opdat de FIE's en de bevoegde autoriteiten hun verplichtingen uit hoofde van de richtlijn kunnen nakomen. Bekeken vanuit de optiek van de bescherming van persoonsgegevens lijkt het noodzakelijk om het soort informatie dat via het verbindingsplatform toegankelijk is te beperken tot het minimumpakket zoals bepaald in artikel 32 bis, lid 3, van de antiwitwasrichtlijn. Overeenkomstig de gegevensbeschermingsregels moet de toegang tot persoonsgegevens in verhouding staan tot hetgeen nodig is voor het bereiken van de in de antiwitwasrichtlijn omschreven doelstellingen. Een soortgelijke benadering wordt toegepast bij de richtlijn ter vergemakkelijking van het gebruik van financiële en andere informatie. In artikel 4, lid 2, van die richtlijn wordt aangegeven dat de aanvullende informatie die de lidstaten opnemen in de gecentraliseerde mechanismen niet toegankelijk en doorzoekbaar is voor de bevoegde autoriteiten.

3.2. Zoekfunctie

Om ervoor te zorgen dat de koppeling van de gecentraliseerde mechanismen meerwaarde voor de gebruikers oplevert, zijn de toepasselijke zoekcriteria van cruciaal belang. De zoekcriteria moeten zodanig worden ontworpen dat de relevante autoriteiten hun taken en onderzoek effectiever kunnen uitvoeren, waarbij de evenredigheid gewaarborgd is en de geldende voorschriften inzake gegevensbescherming worden geëerbiedigd.

Er moet worden nagedacht over de vraag wie gemachtigd wordt tot het uitvoeren van zoekopdrachten (partijen uit de particuliere of uit de openbare sector) en over de vraag met welke gegevens de persoon die de zoekopdracht uitvoert verondersteld kan worden al dan niet bekend te zijn. De vereiste dat de zoekopdracht gegevens dient te bevatten waarmee de zoekende persoon waarschijnlijk niet bekend is, kan effectieve zoekopdrachten bemoeilijken of onmogelijk maken. Verder wordt opgemerkt dat er gevallen zijn waarin een financiële inlichtingeneenheid of een rechtshandhavingsautoriteit uit de ene lidstaat niet op de hoogte is van de geboortedatum of het nationaal identificatienummer van een onderdaan van een andere lidstaat. Als de koppeling ook voor dergelijke aanvullende informatie in de gecentraliseerde systemen gaat gelden, is het belangrijk om te bepalen of het mogelijk moet worden om aan de hand van dergelijke aanvullende informatie zoekopdrachten uit te voeren.

De soorten gegevens die het minimumpakket aan informatie in artikel 32 bis, lid 3, van de antiwitwasrichtlijn vormen, kunnen als zoekcriteria worden overwogen. Hierdoor beantwoordt het verbindingssysteem aan de oorspronkelijke doeleinden van de gecentraliseerde mechanismen. Er zijn extra waarborgen nodig om treffers te kunnen verifiëren (met name in gevallen waarin de zoekopdracht meerdere resultaten oplevert).

De toepasselijke voorwaarden voor de modaliteiten van de zoekopdrachten zijn bepalend voor de effectiviteit van het gebruik van de gekoppelde databanken. De mogelijkheid tot het uitvoeren van zogeheten "fuzzy searches" (zoekopdrachten met veel resultaten, zelfs als een zoekterm verkeerd gespeld of onvolledig is) levert meer treffers op en vergroot de kans dat de gezochte informatie met een zoekopdracht kan worden gevonden, hoewel dit tot zorgen omtrent de gegevensbescherming kan leiden aangezien persoonsgegevens kunnen worden vrijgegeven waarop de zoekopdracht eigenlijk geen betrekking had. Door de vereiste van een exacte match, daarentegen, worden de risico's op onnodige openbaarmaking van persoonsgegevens verkleind, maar groeit de kans dat de zoekmachine de gezochte informatie negeert (indien de spelling van de zoekterm afwijkt of andere transliteratieregels worden toegepast).

De mogelijkheid tot het uitvoeren van "fuzzy searches" leidt tot een lager gebruik van automatische valideringsprocedures en zodoende tot geen of minder verkeerde treffers, maar ook tot een lagere operationele waarde van het systeem. Bij gebruik van "fuzzy searches" moeten andere middelen worden overwogen om het risico op "hengelen naar informatie" te verkleinen, bijvoorbeeld zoals in IRI, waarin sprake is van een bovengrens aan het aantal resultaten dat wordt getoond.

3.3. Governancestructuur en verantwoordelijkheid voor onderhoud

In het geval van BRIS, IRI, LRI en Ecris zijn de diverse diensten van de Europese Commissie *verantwoordelijk voor het onderhoud van het IT-systeem*, wat wil zeggen dat zij voor de beschikbaarheid van de verbindingscomponent moeten zorgen en dat de kosten voor het opzetten en onderhouden ervan voor hun rekening zijn. Vooralsnog wordt e-Codex onderhouden door een consortium van lidstaten (eDelivery van de CEF valt onder de bevoegdheid van de Europese Commissie). In het geval van Eucaris ligt de verantwoordelijkheid bij de 28 lidstaten en de deelnemende derde landen, terwijl Ebocs eigendom is van de European Business Registry Association (EBRA). Aangezien deze IT-systemen nationale databanken met elkaar verbinden, ligt de verantwoordelijkheid voor het onderhoud en de toegankelijkheid ervan bij de lidstaten.

Ten aanzien van de *governancestructuur* voor een systeem dat databanken aan elkaar koppelt, moeten de bevoegdheden betreffende de besluitvorming en operationele kwesties zo worden georganiseerd dat zij de belangen van de nationale componenten dienen.

Bij BRIS fungeert het stuurcomité van BRIS als het interne forum van de Commissie voor de beleidsbeslissingen, het toezicht en het beheer ten aanzien van BRIS, terwijl de deskundigengroep op het gebied van het vennootschapsrecht en bedrijfsregisters (Company Law Expert Group – Business Registers; CLEG-BRIS) dienst doet als forum voor

samenwerking op beleidsniveau tussen de betrokken actoren. Een soortgelijk onderscheid tussen beleidsvorming en operationele structuren is waarneembaar bij Eucaris, waar de uit hoge vertegenwoordigers van overheidsinstanties bestaande algemene vergadering het te volgen beleid vaststelt, de begroting en de jaarlijkse bijdragen goedkeurt en het systeembeheer organiseert.

3.4. Verantwoordelijkheid voor de verwerking

De verantwoordelijkheid voor het onderhoud van het IT-systeem staat los van de kwestie aangaande de *verantwoordelijkheid vanuit de optiek van gegevensbescherming*. Volgens de algemene verordening gegevensbescherming[23] is de verwerkingsverantwoordelijke een natuurlijke persoon of rechtspersoon die alleen of samen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt en de verantwoordelijkheid voor de verwerking van persoonsgegevens draagt. De verantwoordelijkheid voor de verwerking is een complexe zaak en bij de beoordeling van de verwerkingsverantwoordelijke spelen tal van factoren, waaronder de vraag wie de gegevens (waar) opslaat.

Wat IRI betreft, geldt dat dit EU-platform alleen de decentrale nationale databanken met elkaar verbindt en dat alle gegevens die op het centrale platform worden weergegeven eenvoudigweg "tijdelijke gegevens" zijn; deze worden niet in de EU-component opgeslagen en evenmin worden de logbestanden van de zoekopdrachten die door gebruikers via de webdienst worden uitgevoerd geregistreerd of in het centrum bewaard. De situatie verschilt enigszins ten aanzien van BRIS, waarin een speciale functie is geïntroduceerd voor de opslag van de belangrijkste profielgegevens van ondernemingen in een centraal onderdeel op Commissieniveau en die door de nationale registers met regelmatige tussenpozen worden bijgewerkt. De centrale databank wordt doorzocht op de oorspronkelijke zoekopdracht, wat een lijst met treffers met de namen van de entiteiten oplevert. De verzoeker kan over een bepaalde entiteit uitvoerige informatie opvragen door de naam in de lijst met treffers te selecteren. Door deze handeling wordt een rechtstreekse koppeling gemaakt met de informatie in de nationale databank.

Wat de mogelijke koppeling met gecentraliseerde mechanismen betreft, moet een IT-systeem worden overwogen waarin door de component voor de gecentraliseerde routing geen persoonsgegevens worden opgeslagen en waarbij alle beslissingen over de middelen en de doeleinden van de gegevensverwerking op nationaal niveau worden genomen. Het doel van de verbindingsdienst is simpelweg om de gegevensverwerking namens de gecentraliseerde mechanismen – die ten aanzien van hun eigen gegevensreeksen verwerkingsverantwoordelijke blijven – te vergemakkelijken.

3.5. Kosten voor opzet en onderhoud

Het opzetten van een systeem voor het koppelen van de nationale gecentraliseerde mechanismen brengt kosten met zich mee voor zowel het opstellen als het onderhouden

[23] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (algemene verordening gegevensbescherming) betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (PB L 119 van 4.5.2016).

ervan. Deze kosten moeten tussen de EU en de lidstaten worden gedeeld. Bij de voorbeelden van de modellen geldt ten aanzien van de kostendeling de regel dat kosten die te maken hebben met de EU-component (voor gecentraliseerde routing, het EU-platform), uit de algemene EU-begroting worden gefinancierd, terwijl de lidstaten de kosten dragen voor het aanpassen van de nationale systemen zodat deze interoperabel zijn met het EU-systeem van onderlinge koppeling. Met de ontwikkeling van de eerste versie van BRIS – die in juni 2017 in gebruik werd genomen en het Europees centraal platform omvatte – was een bedrag van ongeveer 1,7 miljoen EUR gemoeid. Voor IRI, dat een eenvoudiger architectuur kent, bedroegen de kosten voor de ontwikkeling van het prototype van het centrale zoeksysteem (IRI 1.0) ongeveer 280 000 EUR terwijl de aanpassing van de centrale zoekfunctie ten behoeve van het opzetten van IRI 2.0 ongeveer 170 000 EUR zal kosten. Bij Ecris belopen de totale kosten voor de invoering van de "referentie-implementatie" (de software voor het uitwisselen van gegevens over strafregisters tussen de lidstaten) 2 050 000 EUR. De jaarlijkse onderhoudskosten van het systeem bedroegen 150 000 EUR. In het geval van Eucaris wordt voor onderhoudsdoeleinden aan alle deelnemende landen een algemene vergoeding van ongeveer 20 000 EUR gevraagd.

De bovenstaande bedragen lijken erop te wijzen dat de kosten voor het opzetten en onderhouden van een EU-breed verbindingssysteem tamelijk laag zijn in verhouding tot de voordelen die een dergelijk project de EU oplevert. De kostenefficiëntie kan worden verbeterd door hergebruik van bestaande capaciteiten (zoals eDelivery-toegangspunten, bouwstenen van de financieringsfaciliteit voor Europese verbindingen, kernvocabulaires van het directoraat-generaal Informatica van de Europese Commissie enz.).

4. Technische specificaties van de systemen, inclusief gegevensbeveiliging

4.6. Gebruikt netwerk en gegevensbeveiliging

De Prüm-dienst van Eucaris en Ecris maken gebruik van de trans-Europese diensten voor telematica tussen overheidsdiensten (Trans European Services for Telematics between Administrations; TESTA), een particulier netwerk dat volledig gescheiden is van het openbare internet. De aangewezen nationale contactpunten hebben toegang tot dit particuliere netwerk. De TESTA-netwerkdienst staat onder beheer van de Commissie en biedt gegarandeerde prestaties en een hoog beveiligingsniveau. Eucaris kan via het openbare internet worden gebruikt, maar deze mogelijkheid wordt momenteel niet benut. Eucaris is met alle EU-instellingen en nationale netwerken verbonden en krijgt de voorkeur bij samenwerking op het gebied van rechtshandhaving waarbij sprake is van gevoelige informatie. De EU-instellingen hebben ook andere beveiligde netwerken ontwikkeld, zoals het gemeenschappelijk communicatienetwerk met gemeenschappelijke systeeminterface (CCN/CSI), die op het terrein van douanebeleid en belastingen wordt gebruikt.

BRIS, IRI, LRI en Ebocs maken gebruik van het openbare internet (met gepaste versleutelingstechnologie voor de gegevens die via het internet worden verzonden). Ten aanzien van de beveiligde uitwisseling van informatie via het openbare internet geldt dat de bouwsteen eDelivery ondernemingen en overheidsdiensten in staat stelt om op

interoperabele, beveiligde, betrouwbare en vertrouwenwekkende wijze elektronische gegevens en documenten in digitale vorm met andere organisaties uit te wisselen. Dit is in overeenstemming gebracht met de definitie van "dienst voor elektronisch aangetekende bezorging" (bekend als "ERDS") in artikel 3, lid 36, van de eIDAS-verordening[24].

Voor de mogelijke koppeling van gecentraliseerde systemen, waarbij aantoonbaar sprake is van gevoelige informatie, kan het gebruik van TESTA worden overwogen. Niettemin moeten ook oplossingen op het vlak van het openbare internet in overweging worden genomen. Vrijwel alle nationale gecentraliseerde systemen maken gebruik van het openbare internet. Vanuit gegevensbeveiliging en -integriteit bekeken, worden de eventuele risico's verkleind doordat het systeem uit decentrale databanken zal bestaan, aangezien decentralisatie en gedistribueerde technologieën als zodanig beter bestand zijn tegen cyberaanvallen vanwege het feit dat het veel moeilijker is om gegevens op grote schaal te beschadigen en het veel eenvoudiger is om gegevens na een incident te herstellen.

4.7. Gecentraliseerde routing

Er bestaan voor IT-systemen twee belangrijke typen architectuur, namelijk de zuiver decentrale systemen en de systemen met een op EU-niveau ingesteld centraal platform of gecentraliseerde routing die dienst doen als "koppeling" tussen de decentrale nationale databanken.

Bij "zuivere gedistribueerde systemen" bestaat er geen EU-platform of -component, maar communiceren alle landen rechtstreeks met elkaar met behulp van gezamenlijk overeengekomen normen voor rechtstreekse peer-to-peeruitwisseling tussen de met elkaar verbonden punten van de lidstaten. Als er een zoekopdracht wordt ingevoerd, wordt deze dus afzonderlijk naar alle andere nationale systemen verstuurd en worden de ontvangen antwoorden via de webinterface van de verzoeker verzameld en getoond. Eucaris, Ecris en e-Codex passen deze technologie toe (en maken gebruik van een gezamenlijk ontwikkelde toepassing).

In "gedistribueerde systemen met gecentraliseerde routing" is er sprake van een gecentraliseerd platform op EU-niveau: één centrale webdienst die op EU-niveau wordt onderhouden en geëxploiteerd en met alle nationale systemen is verbonden. Gebruikers voeren zoekopdrachten uit in de centrale webdienst, die vervolgens de informatie uit de nationale databanken haalt. BRIS, Ebocs en IRI maken gebruik van deze technologie[25].

Een oplossing met gecentraliseerde routing kan, bekeken vanuit het oogpunt van connectiviteit, makkelijker uit te voeren zijn. In het geval van één enkel platform hoeft elke

[24] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PB L 257 van 28.8.2014, blz. 73).

[25] Er bestaan alternatieven voor een gecentraliseerde component. De publisher van metagegevens voor diensten van eDelivery van de CEF biedt deelnemers aan de infrastructuur voor berichten de mogelijkheid om op dynamische wijze elkaars capaciteiten te ontdekken (juridisch, organisatorisch en technisch). Vanwege deze gedistribueerde architectuur moet iedere deelnemer over een unieke ID beschikken. Een centrale component met de naam "Service Metadata Locator" gebruikt deze ID's voor het aanmaken van URL's die, als ze zijn omgezet, de eDelivery-toegangspunten doorleiden naar de specifieke informatie over de deelnemer.

lidstaat slechts één verbinding tussen het nationale systeem en dit gecentraliseerde platform te maken en te onderhouden. Als er geen "echt" gecentraliseerd platform bestaat, moet elke lidstaat daarentegen verbindingen maken met alle andere nationale systemen van de lidstaat en deze testen en onderhouden (de Prüm-dienst van Eucaris, bijvoorbeeld, telt momenteel bijna 756 verbindingen). Een zuiver gedistribueerd systeem moet zijn opgewassen tegen een veelvoud aan verbindingen, wat de problemen ten aanzien van beheer, controle en audit kan vergroten. Niettemin bestaan er technische oplossingen voor de problemen die het beheer van een groot aantal mogelijke verbindingen met zich meebrengt. Tegelijkertijd moet er voldoende aandacht zijn voor het feit dat in een systeem met gecentraliseerde routing de gecentraliseerde component tot het zwakke punt van het hele systeem kan uitgroeien.

4.8. Protocol voor gegevensuitwisseling

BRIS en e-Codex maken gebruik van de oplossing eDelivery van de CEF, terwijl IRI 2.0 van zowel eDelivery als SOAP-communicatie[26] gebruikmaakt. De Prüm-dienst van Eucaris alsook Ebocs maken gebruik van op SOAP gebaseerde interfaces. LRI past RESTful-webdiensten toe[27].

De bouwsteen eDelivery van de CEF helpt gebruikers bij het onderling op beveiligde, betrouwbare en vertrouwenwekkende wijze uitwisselen van elektronische gegevens. De oplossing eDelivery van de CEF is gebaseerd op een gedistribueerd model met de naam "4-corner model" waarbij de back-end systemen van de gebruikers niet rechtstreeks onderling gegevens uitwisselen maar dat via toegangspunten doen. Deze toegangspunten kennen dezelfde technische specificaties en kunnen daarom met elkaar communiceren. Een ander voordeel van eDelivery is dat het de beveiliging regelt van de gegevens die tussen de verschillende toegangspunten worden uitgewisseld, zonder dat er ontwikkeling op maat nodig is. Als gevolg hiervan kunnen gebruikers die overstappen op eDelivery van de CEF eenvoudig en veilig gegevens uitwisselen, zelfs als hun IT-systemen onafhankelijk van elkaar ontwikkeld zijn. Het eDelivery-model is bijzonder nuttig voor het maken van verbinding met meerdere back-end systemen en diverse functies kunnen juist worden gecentraliseerd. Bij gebruik van deze technische oplossing moeten de lidstaten (en in het geval van gecentraliseerde routing eventueel de Commissie) een eDelivery-toegangspoort op hun eigen niveau inschakelen. Zij kunnen hun bestaande, voor andere diensten ontwikkelde toegangspoorten hergebruiken (hetgeen bijdraagt aan de kosteneffectiviteit van de oplossing). Er bestaat een compatibele, door het directoraat-generaal Informatica van de Europese Commissie ontwikkelde software-oplossing die overeenkomstig een openbare licentie van de Europese Unie (EUPL) gratis wordt aangeboden. Doorgaans is echter enige aanpassing en ontwikkeling vereist. Het eDelivery-model is geënt op asynchrone communicatie, hetgeen per definitie bepaalde vertragingen in de prestaties oplevert (doorgaans 3-10 seconden). Er bestaat ten aanzien van de CEF-bouwstenen een algemeen EU-beleid, dat gericht is op convergentie van de diverse systemen die op de verschillende EU-beleidsterreinen zijn ontwikkeld.

[26] SOAP staat voor "Simple Object Access Protocol".
[27] Representational state transfer (REST) is een software-architectuur die een aantal voorwaarden definieert die bij het opzetten van webdiensten moeten worden gebruikt.

Indien gebruik wordt gemaakt van synchrone SOAP, die communicatie via een beveiligingslaag mogelijk maakt, wordt meestal voor een eenvoudigere architectuur gekozen, met als doel zo hoog mogelijke prestaties. In vergelijking met SOAP vertegenwoordigt de RESTful-architectuur een nieuwere oplossing en het komt steeds vaker voor dat SOAP door REST-technologie wordt vervangen. Bij benaderingen op basis van zowel eDelivery als SOAP dan wel REST is het vertrouwen meestal gebaseerd op digitale certificaten en worden diverse controles uitgevoerd.

Over de toekomstige koppeling van gecentraliseerde mechanismen wordt hier opgemerkt dat in de CEF, als er sprake is van bilaterale uitwisselingen tussen de decentrale nationale databanken, gebruik wordt gemaakt van eDelivery, terwijl in de systemen waarin de communicatie uitsluitend tussen een nationale databank en het centrale platform verloopt, de op SOAP gebaseerde interface (of RESTful) volstaat.

4.9. Functioneren in een meertalige omgeving en semantische interoperabiliteit

Alle beoordeelde systemen functioneren in een meertalige omgeving, met uitzondering van Ebocs, dat momenteel in drie talen functioneert en volgens plan op de lange termijn in alle talen zal functioneren. In het geval van BRIS wordt de transliteratie op EU-niveau uitgevoerd, terwijl dat bij IRI, LRI en Eucaris op nationaal niveau gebeurt. Ten aanzien van semantische interoperabiliteit (verklarende woordenlijsten) geldt dat voor een toekomstige koppeling van gecentraliseerde mechanismen geen specifiek lexicon is vereist, aangezien het minimumpakket informatie niet uit nationale concepten maar uit persoonsgegevens bestaat, zoals een naam, een eenduidig identificatienummer (bv. nationale ID-nummers) en een IBAN-nummer. Een gemeenschappelijke interpretatie in alle nationale systemen is cruciaal, met name vanwege het feit dat de nationale gecentraliseerde mechanismen geen informatie over entiteiten in de EU en in derde landen bevatten. De regels voor transliteratie van het Schengeninformatiesysteem kunnen in dit verband als nuttig voorbeeld dienen.

Volgens het Europese interoperabiliteitskader verwijst het semantische aspect naar de betekenis van gegevenselementen en hun onderlinge verbanden. Dit omvat de ontwikkeling van lexicons en schemata ter beschrijving van de gegevensuitwisseling en zorgt ervoor dat de met elkaar communicerende partijen de gegevenselementen op dezelfde manier interpreteren.

Voor het systeem om bankenregisters met elkaar te verbinden is het nodig gegevens tussen verschillende databanken uit te wisselen, die ieder hun eigen gegevensmodellen en semantische normen hebben. Er moeten gemeenschappelijke semantische normen worden opgesteld, hetzij in de systemen geïntegreerd of als toewijzingslaag tussen de verschillende normen in de lidstaten. Voordat er een nieuwe semantische norm wordt ontwikkeld, moet evenwel hergebruik van reeds bestaande normen worden overwogen.

De door het ISA2-programma ontwikkelde kernvocabulaires (onderneming, locatie, persoon en andere) zijn vereenvoudigde, herbruikbare en uitbreidbare gegevensmodellen die voor dit doel kunnen worden gebruikt. Bij diverse oplossingen voor het koppelen van basisregisters, zoals BRIS, worden sommige normen al opnieuw gebruikt (bijvoorbeeld het basisvocabulaire ondernemingen).

5. Vervolgstappen

Dit verslag bevat een aantal punten waarmee bij een eventuele koppeling tussen registers van bankrekeningen en systemen voor gegevensontsluiting rekening moet worden gehouden en laat zien dat de koppeling van die gecentraliseerde mechanismen in technisch opzicht haalbaar is. Een dergelijk systeem zou mogelijk kunnen bestaan uit een decentraal systeem met een gemeenschappelijk platform op EU-niveau. Hiervoor kan gebruik worden gemaakt van technologie die door de Europese Commissie in het kader van de diverse onderzochte modellen reeds is ontwikkeld.

De afgelopen jaren zijn diverse systemen overgegaan op hergebruik van gemeenschappelijke bouwstenen. Deze bouwstenen vormen in wezen een reeks bekende normen en technische specificaties die bij terugkerende uitdagingen, zoals de beveiligde uitwisseling van informatie, kunnen worden toegepast. In het huidige digitale beleid van de Commissie, waartoe de lidstaten zich in de Verklaring van Tallinn inzake e-overheid hebben verbonden, wordt aanbevolen om consequent gebruik te maken van deze bouwstenen[28]. Een toekomstige koppeling van nationale gecentraliseerde automatische mechanismen kan het gebruik van dezelfde bouwstenen stimuleren, zodat de totstandkoming en de afstemming daarvan op de relevante EU-verordeningen, zoals eIDAS, wordt bespoedigd.

Gezien het feit dat een toekomstige EU-brede koppeling van gecentraliseerde mechanismen zal zorgen voor snellere toegang tot financiële informatie en voor vergemakkelijking van de grensoverschrijdende samenwerking tussen bevoegde autoriteiten, is de Commissie voornemens nader overleg te plegen met belanghebbenden alsook met de financiële inlichtingeneenheden, rechtshandhavingsinstanties en bureaus voor de ontneming van vermogensbestanddelen als mogelijke “eindgebruikers” van een eventueel verbindingssysteem.

[28] In Tallinn is op 6 oktober 2017 de “Verklaring e-overheid” door alle lidstaten van de Europese Unie en de EVA-landen ondertekend. De tekst van de verklaring is te raadplegen op http://ec.europa.eu/newsroom/document.cfm?doc_id=47559